

## REMARKS

Claims 1-7, 9-29, 31-32, 35-38, and 40-44 are pending. The rejections of the claims are respectfully traversed in light of the amendments and following remarks and reconsideration is requested.

### Rejection Under 35 U.S.C. § 103

Claims 1-7, 9-17, 19-29, 32-32, 35-38, and 40-44 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Sims, III (U.S. Patent No. 6,550,011 hereinafter "Sims") in view of Naim (U.S. Patent No. 6,779,115).

In rejecting the claims, the Examiner writes in part:

Sims does not explicitly disclose but Naim discloses a user key device associated with a user, the user key device detachably connected to the processing device, accessible by the user [program], and configured to restrict the use of the data object to the user using a user key (Naim, col. 4, lines 45-51). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching of Naim's user key device on a removable smart card for decrypting data content with Sims' teaching of decrypting content with device key in order to allow the purchased digital goods to be played on different devices or protects the digital goods from loss due to device failure or the need to upgrade the devices (Naim, col. 4, lines 35-45).

However, Naim discloses the following:

Because the encrypted music files are associated with the card and not with the disk, when data is lost due, for example, to a disk crash on one portable player, the music files may be recovered from back-up copies and played on other devices by, for example, detaching the card from the first device and inserting it in a second portable device. (Naim, col. 4, lines 52-57) (emphasis added).

The exemplary embodiment of the invention has two main elements, a portable smart card or smart card that allows the digital data to be decrypted on any device that supports the smart card or chip, and the use of public and private keys . . . to establish a channel with one or more vendors through which music may be purchased and to allow purchasers to protect their investment in purchased encrypted music by tying the encrypted music not to a hard disk or other data storage medium but to a smart card or smart card that can be used with any device that supports the smart card or chip . . . (Naim, col. 5, lines 39-50) (emphasis added).

Thus, Naim discloses a smart card for decrypting encrypted digital data but teaches away from tying encrypted digital data to a hard disk or other data storage medium. Otherwise, the advantages (and intended function of the invention) taught in Naim for allowing the purchased digital music to be played on different devices or protecting the digital music from loss due to hard disk crashed or the need to upgrade the portable device would be lost. Accordingly, there is no motivation in Naim to be combined with a device key of Sims, and instead Naim teaches away from a combination of a user key and a machine key as taught in the present invention.

In contrast, the present invention provides that the “user key device is preferably a removable, portable device that connects to the user data processor and provides encryption, decryption, and authentication functionality for the user” and that the use of a data object is restricted “to a particular user and a particular data processor through the use of additional layers of encryption.” (Specification as filed, page 3, lines 6-15)

In particular, Claim 1 recites a data processor, comprising “a user key device associated with a user, the user key device detachably connected to the processing device, accessible by the user program, and configured to restrict the use of the data object to the user using a user key” and “a machine key device connected to and associated with the processing device and accessible by the user program, the machine key device configured to restrict the use of the data object to the user data processor using a machine key.”

Similarly, Claim 25 recites a method, comprising “encrypting the data object such that decryption requires the user program key and the machine key” and “encrypting the data object such that decryption also requires the user key.”

Similarly, Claim 32 recites a method, comprising “creating a machine control element configured to cause the user program to restrict use of the data object to the particular user data processor by authenticating the particular user data processor based upon at least the machine key and by at least communicating with the machine key device” and “creating a user control element configured to cause the user program to restrict use of the data object to the particular user by authenticating the particular user based upon at least the user key and by at least communicating with the user key device.”

Similarly, Claim 38 recites a method, comprising “encrypting the data object such that decryption requires the user program key and the machine key”, “decrypting the data object

using the user program key and the machine key”, “encrypting the data object such that decryption also requires the user key”, and “decrypting the data object using the user key.”

Similarly, Claim 44 recites “a secure data package . . . comprising a controlled portion of the data object, the controlled portion encrypted such that decryption requires both a user program key and a machine key, . . . wherein the controlled portion is additionally encrypted such that decryption requires a user key, wherein the user key is maintained by a user key device associated with a particular user and detachably connected to the processing device.”

Therefore, because Sims in view of Naim does not disclose or suggest all the limitations of independent Claims 1, 25, 32, 38, and 44, Claims 1, 25, 32, 38, and 44 are patentable over Sims in view of Naim.

Claims 2-7, 9-17, and 19-24 are dependent on Claim 1, Claims 26-29 and 31 are dependent on Claim 25, Claims 35-37 are dependent on Claim 32, Claims 40-43 are dependent on Claim 38, and contain additional limitations that further distinguish them from Sims in view of Naim. Therefore, Claims 2-7, 9-17, 19-24, 26-29, 31, 35-37, and 40-43 are patentable over Sims in view of Naim for at least the same reasons stated above with regard to Claims 1, 25, 32, and 38.

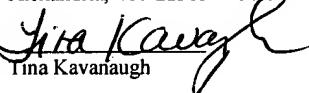
Claim 18 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Sims in view of Naim and further in view of Keeler, Jr. et al. (U.S. Patent No. 6,502,130 hereinafter “Keeler”). Keeler is directed toward a “system and method which collects dynamic connectivity data from an area network interconnecting multiple computing devices” (Keeler, Abstract) and does not remedy the deficiencies of Sims and Naim noted above. Claim 18 is also dependent on Claim 1 and contains additional limitations that further distinguish it from Sims in view of Naim and further in view of Keeler. Therefore, because neither Sims nor Naim nor Keeler, alone or in combination, disclose or suggest all the limitations of Claim 18, Claim 18 is patentable over Sims in view of Naim and further in view of Keeler for at least the same reasons stated above with respect to Claim 1.

## CONCLUSION

For the above reasons, Applicant believes pending Claims 1-7, 9-29, 31-32, 35-38, and 40-44 are now in condition for allowance and allowance of the application is hereby solicited. If the Examiner has any questions or concerns, the Examiner is hereby requested to telephone Applicants' Attorney at (949) 752-7040.

### Certificate of First Class Mail

I hereby certify that this paper is being sent by First Class Mail to the U.S. Patent and Trademark Office, Mail Stop RCE, Box 1450, Alexandria, VA 22313-1450 on the date shown below.

  
Tina Kavanaugh

June 7, 2005

Respectfully submitted,



David S. Park  
Attorney for Applicant(s)  
Reg. No. 52,094